

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Missouri

**In the Matter of the Search of** )  
 Information associated with "glennjwill2011@icloud.com;" )  
 "lexiiv89@gmail.com," "lexiiv89@icloud.com;" ) Case No. 4:22 MJ 26 (DDN)  
 "lexiv89@icloud.com;" "alexandriav89@icloud.com;" )  
 "ekingwilliams@icloud.com;" elijahkingw@icloud.com that ) SUBMITTED TO THE COURT AND  
 is stored at premises controlled by Apple, Inc. ) SIGNED BY RELIABLE ELECTRONIC MEANS

**APPLICATION FOR A SEARCH WARRANT**

I, DREW POLAN, a federal law enforcement officer or an attorney for the government request  
 a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

**SEE ATTACHMENT A**

located in the NORTHERN District of CALIFORNIA, there is now concealed

**SEE ATTACHMENT B**

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☐ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section**Offense Description*

Title 21, U.S.C., §§ 846, 841(a)(1)

Conspiracy to possess with intent to distribute controlled  
 substance(s)

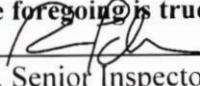
The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested  
 under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

**I state under the penalty of perjury that the foregoing is true and correct.**

  
 Drew Polan, Senior Inspector  
 United States Marshals Service

*Printed name and title*

Sworn to, attested to, and affirmed before me via  
 reliable electronic means pursuant to Federal Rules of  
 Criminal Procedure 4.1 and 41.

Date: February 2, 2022

/s/ **David D. Noce**

*Judge's signature*

City and State: St. Louis, MO

**DAVID D. NOCE, U.S. Magistrate Judge**

*Printed name and title*

AUSA: STEPHEN CASEY

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with:

"glennjwill2011@icloud.com;" "lexiiv89@gmail.com;" "lexiiv89@icloud.com;"  
"lexiv89@icloud.com;" "alexandriav89@icloud.com;" "ekingwilliams@icloud.com;"  
"elijahkingw@icloud.com"

(the "accounts") that are stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be disclosed by Apple**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers

(“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the accounts from May 1, 2021 to present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the from May 1, 2021 to present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and

query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

**The Provider is hereby ordered to disclose the above information to the government within 14 days of the date of this warrant.**

## **II. Information to be seized by the United States**

All information described above in Section I that constitutes the location of Glenn Williams, a federal fugitive, from May 1, 2021 to the present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Information which may reasonably assist the United States Marshals Service in identifying linked devices, IP addresses, third party application data, location information, and other information which would be relevant in assisting in the location and arrest of Glenn Williams, a federal fugitive;

b. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

c. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of each account access, use and events relating to the accounts subscriber(s);

d. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

e. Records and things evidencing the use of the Internet to communicate with servers, including:

i. records of Internet Protocol addresses used and records of Internet activity;

ii. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

f. Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crime under investigation;

g. Evidence indicating the geographic location of the cellular device at times relevant to the investigation;

h. The identity of the person(s) who sent to and/or received communications from the account that help reveal their whereabouts.

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH	)	
OF INFORMATION ASSOCIATED WITH	)	No. 4:22 MJ 26 (DDN)
"glennjwill2011@icloud.com"	)	
"lexiiv89@gmail.com"	)	
"lexiiv89@icloud.com"	)	FILED UNDER SEAL
"lexiv89@icloud.com"	)	
"alexandriav89@icloud.com"	)	
"ekingwilliams@icloud.com"	)	SUBMITTED TO THE COURT AND
"elijahkingw@icloud.com"	)	SIGNED BY RELIABLE ELECTRONIC
STORED AT PREMISES CONTROLLED	)	MEANS
BY APPLE, INC.	)	

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

Senior Inspector Drew Polan, United States Marshals Service (USMS), being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41 to require Apple Inc. (hereafter "Apple"), an electronic communications service/remote computing service provider, to disclose to the United States records and other information, including the contents of communications, associated with the above-listed Apple ID that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I, Drew Polan, am a Senior Inspector with the United States Marshals Service ("USMS") and, as such, I am charged with enforcing all laws in all jurisdictions of the United States, its territories and possessions. My current duty assignment is in the Investigative

Operations Division, Organized Crime and Gangs Branch. My primary duty and assignment obligates me to investigative, locate, and apprehend fugitives, and support fugitive investigative efforts on behalf of the USMS. I have been employed with the USMS for 13 years and have a cumulative total of 16 years of experience as a federal law enforcement officer. I have been assigned to fugitive investigations for more than 10 years and have been the lead investigator in more than 700 fugitive investigations, in addition to providing investigative assistance in scores of other cases. My experience also includes the utilization of various electronic surveillance measures, empowered through legal process, in over 100 investigations.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. The United States Marshals Service has probable cause to believe that the iCloud accounts described herein are currently being used by Glenn WILLIAMS who is charged with conspiracy to distribute methamphetamine, heroin, and fentanyl, in violation of Title 21, United States Code, Section 846 and possessing a firearm in furtherance of a drug trafficking crime in violation of Title 18, United States Code, Section 924(c), in Case No. 4:21-CR-00554, and whose whereabouts are currently unknown.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that information regarding the whereabouts of Glenn WILLIAMS will be found in the locations described in Attachment A for evidence described in Attachment B.

### **JURISDICTION**

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **LOCATIONS TO BE SEARCHED**

7. The locations to be searched are:

“glennjwill2011@icloud.com”  
“lexiiv89@gmail.com”  
“lexiiv89@icloud.com”  
“lexiv89@icloud.com”  
“alexandriav89@icloud.com”  
“ekingwilliams@icloud.com”  
“elijahkingw@icloud.com”  
(hereinafter referred to as “the account(s)”)

located at a premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

### **BACKGROUND INFORMATION RELATING TO APPLE ID AND iCloud<sup>1</sup>**

8. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

---

1. The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at [https://www.apple.com/business/docs/iOS\\_Security\\_Guide.pdf](https://www.apple.com/business/docs/iOS_Security_Guide.pdf), and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

9. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and

presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

10. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

11. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-

party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

12. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

13. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases from App Store and iTunes Store, “call invitation logs” for FaceTime calls, “query logs” for iMessage, and “mail logs” for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

14. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

15. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging

service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

16. In some cases, account users will communicate directly with Apple about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Apple typically retains records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

### **PROBABLE CAUSE**

Law enforcement, including the United States Marshals Service (USMS), is conducting a fugitive investigation for Glenn WILLIAMS.

17. WILLIAMS was charged in Case No. 4:21-CR-00554 with conspiracy to distribute methamphetamine, heroin, and fentanyl, in violation of Title 21, United States Code, Section 846, and possessing a firearm in furtherance of a drug trafficking crime in violation of Title 18, United States Code, Section 924(c). The indictment was returned by the Grand Jury, and an arrest warrant issued for WILLIAMS, on October 13, 2021. Efforts to arrest WILLIAMS were unsuccessful, and a fugitive investigation was initiated.

18. On October 19, 2021, USMS investigators conducted an interview of Alexandria VENOYA-WILLIAMS, WILLIAMS' estranged wife and the mother of his two minor children. During the interview, VENOYA-WILLIAMS indicated she and WILLIAMS were estranged but indicated WILLIAMS was a loving father and, despite not knowing his whereabouts, believed WILLIAMS would maintain lines of communications where the couple's two minor children. VENOYA-WILLIAMS also indicated the children both had electronic devices.

19. Subsequent interviews conducted by USMS in October 2021 of WILLIAMS' mother and in December 2021 of WILLIAMS' brother failed to reveal information concerning WILLIAMS' whereabouts. During the interview of WILLIAMS' brother (Geordan REED), REED indicated he was told by family members WILLIAMS' was a fugitive.

20. Additionally, WILLIAMS stated he was very close with his children during a pre-indictment interview with the DEA and Postal Inspectors.

21. USMS investigation later determined that, in December 2021, VENOA-WILLIAMS and the two minor children moved from San Bernardino County, California, to Las Vegas, Nevada. The move was not characteristic of VENOA-WILLIAMS, who had previously been a long time San Bernardino resident and most of her relatives lived in California. January 2022 surveillance by the USMS in Nevada confirmed VENOA-WILLIAMS and the two children were living at an apartment in Las Vegas, but WILLIAMS was not seen during the surveillance. The children were un-enrolled in San Bernardino-area schools in December 2021, and enrolled in a Las Vegas elementary school effective in January 2022.

22. On January 12, 2022, I obtained via subpoena from Apple information related to iCloud accounts associated to WILLIAMS, as well as accounts associated to residences associated with WILLIAMS, and telephone numbers historically attributable to WILLIAMS, VENOA-WILLIAMS, and the couple's children.

23. Information provided as part of the production by Apple included Internet Protocol ("IP") login activity and subscriber details associated to several iCloud accounts, including:

"glennjwill2011@icloud.com"  
"lexiiv89@gmail.com"  
"lexiiv89@icloud.com"  
"lexiv89@icloud.com"  
"alexandriav89@icloud.com"

“ekingwilliams@icloud.com”  
“elijahkingw@icloud.com”

24. In reviewing the data, I and other investigators noted the presence of several overlapping “verified phone” numbers on the accounts. Specifically, telephone number (818) 245-2556 (previously determined by USMS investigators to be VENOYA-WILLIAMS’ longstanding cellular telephone number) was listed as the verified phone for the iCloud accounts “alexandriav89@icloud.com,” “ekingwilliams@icloud.com,” “elijahkingw@icloud.com,” “lexiiv89@gmail.com,” and “lexiiv89@icloud.com.” Additionally, “Facetime/iMessage Phone” numbers were listed for “elijahkingw@icloud.com” (442-343-6816) and “lexiiv89@icloud.com” (442-343-6815).

25. Account “elijahkingw@icloud” was created on August 3, 2021 and “lexiiv89@icloud” was created on July 27, 2021. Of note is DEA and USPIS investigators representations to USMS investigators concerning their contact with WILLIAMS during the underlying drug investigation, wherein investigators communicated regularly with WILLIAMS after the execution of a search warrant in May 2021, until WILLIAMS abruptly stopped communicating in July 2021. Toll data for the cellular telephone associated with WILLIAMS at the time showed call activity ceasing in mid-July 2021. Since July 2021, neither DEA, USPIS, nor USMS investigators have been able to ascertain an active telephone number for WILLIAMS, nor his location.

26. A review of IP login activity in December 2021 and January 2022 of the aforementioned accounts showed several suspicious logins. Specifically, on January 11, 2022, an IP address located in San Bernardino County, California accessed account “ekingwilliams@icloud.com”; while “elijahkingw@icloud.com,” “alexandriava89@icloud,”

“lexii89@icloud.com,” and “glennjwill2011@icloud.com” all have logins from IP addresses in Las Vegas, Nevada.

27. Also on January 11, 2022, “glennjwill2011@icloud.com” had IP login activity in California and Nevada less than 3 hours apart. While it was conceivable that a person could drive between the locales on the same day, the IP logins were associated to an account believed to be the moniker of Glenn Williams Jr., who is a 10-year-old child. Moreover, as the surveillance of VENOYA-WILLIAMS in Las Vegas, Nevada only noted the presence of VENOYA-WILLIAMS and the two children, it is unlikely VENOYA-WILLIAMS left the two children unattended during interstate travel.

28. This login activity is indicative of multiple devices being linked to the same iCloud accounts. As such, it is believed that in the absence of traditional telephone calls between WILLIAMS, his minor children, and possibly his estranged wife, WILLIAMS is likely using applications and other internet-based communications services to communicate with his family, and that information is stored in the content retained by Apple. Additionally, several accounts with minor derivations (for example, the Grand Jury subpoena revealed the presence of accounts for “lexiiv89@gmail.com”, “lexiiv89@icloud.com”, and “lexiv89@icloud.com” are suggestive of VENOYA-WILLIAMS (whose nickname is known as “Lexi”) creating multiple accounts which are, in turn, accessed across several platforms.

29. In my training and experience, some fugitives avoid traditional telephonic communication with friends and relatives, believing it easy for law enforcement to track their whereabouts via telephone. A trend by some fugitives is the use of web-based applications and communication services to facilitate communication with friends and relatives, while simultaneously limiting their attribution of calls and text messages over regular service providers.

The kinds of data that may be stored in an Apple ID account can provide information concerning new or additional cellular devices, Internet Protocol addresses, email addresses, location information, downloaded apps, and other information which may be utilized in furtherance of identifying Williams' location for purposes of arrest.

### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

30. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the United States copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

### **CONCLUSION**

31. Based on the forgoing, I request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

32. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

33. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents

discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under the penalty of perjury that the foregoing is true and correct.

  
\_\_\_\_\_  
DREW POLAN  
SENIOR INSPECTOR - USMS

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 this 2nd day of February, 2022.

/s/ David D. Noce  
\_\_\_\_\_  
DAVID D. NOCE  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with:

"glennjwill2011@icloud.com;" "lexiiv89@gmail.com;" "lexiiv89@icloud.com;"  
"lexiv89@icloud.com;" "alexandriav89@icloud.com;" "ekingwilliams@icloud.com;"  
"elijahkingw@icloud.com"

(the "accounts") that are stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Apple**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the accounts from May 1, 2021 to present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the from May 1, 2021 to present, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and

query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

**The Provider is hereby ordered to disclose the above information to the government within 14 days of the date of this warrant.**

## **II. Information to be seized by the United States**

All information described above in Section I that constitutes the location of Glenn Williams, a federal fugitive, from May 1, 2021 to the present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Information which may reasonably assist the United States Marshals Service in identifying linked devices, IP addresses, third party application data, location information, and other information which would be relevant in assisting in the location and arrest of Glenn Williams, a federal fugitive;

b. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

c. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of each account access, use and events relating to the accounts subscriber(s);

d. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

e. Records and things evidencing the use of the Internet to communicate with servers, including:

i. records of Internet Protocol addresses used and records of Internet activity;

ii. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

f. Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crime under investigation;

g. Evidence indicating the geographic location of the cellular device at times relevant to the investigation;

h. The identity of the person(s) who sent to and/or received communications from the account that help reveal their whereabouts.